

From: [Sonmez Turan, Meltem \(Fed\)](#)
To: [Foti, James \(Fed\)](#); [Chen, Lily \(Fed\)](#)
Cc: [Kerman, Sara J. \(Fed\)](#)
Subject: RE: SHA-3 Development
Date: Monday, September 13, 2021 10:15:52 AM

Thanks for the information Jim. This is helpful.

From: Foti, James (Fed) <james.foti@nist.gov>
Sent: Monday, September 13, 2021 10:12 AM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: SHA-3 Development

Hi Meltem-

You should be aware that before submitting an article to JRES for their consideration, it must go through the ERB review process and be approved by them first before you can submit to JRES.

Honestly, I think it would be highly unlikely to get a quality paper drafted and through ERB within the next 17 days. Remember that you're also going to be competing (in ERB) with other publications for review time from division and ITL management, during the final 2.5 weeks of the FY.

The deadlines for JRES (submissions by 9/30, and final JRES article published by 12/31) are solid and cannot be changed.

As far as other venues go, it depends on the style of the article. But NISTIR is the most obvious candidate IMO, given that's where we've published our reports on rounds of the SHA-3, Lightweight Crypto, and PQC projects. An overview of the entire SHA-3 project would seem to fit there, too.

Jim

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Monday, September 13, 2021 9:49 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>
Subject: RE: SHA-3 Development

It's a good idea to contact Bill and Shu-jen. I will try to prepare a draft outline within 2-3 days, to initiate the discussions.

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, September 13, 2021 9:46 AM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>; Foti, James (Fed) <james.foti@nist.gov>

Subject: Re: SHA-3 Development

Hi, Meltem,

Regardless whether we will submit to the last issue of the Journal, we will start to prepare the draft. It is great if you can start an outline. Shall we contact Bill and Shu-jen to see if they are interested?

Thanks,
Lily

From: "Sonmez Turan, Meltem (Fed)" <meltem.turan@nist.gov>

Date: Monday, September 13, 2021 at 9:39 AM

To: Lily Chen <lily.chen@nist.gov>, "Foti, James (Fed)" <james.foti@nist.gov>

Subject: RE: SHA-3 Development

Jim,

Couple of weeks ago, we received an email saying that the final issue of *Journal of Research of NIST* accepts submissions through September 30, 2021. Since this is going to be an important last issue, it might be a good opportunity publish a paper that describes the *development of SHA-3*. Do you know if there is a possibility of extending the deadline? Or are you aware of other venues that might be suitable for this SHA-3 publication?

Lily,

We have the status reports that make it easier to compile the information we need, but I agree preparing a good paper in two weeks is tight. I can propose a draft outline, just in case we decide to submit. If not, the outline can later be used by our group. Would that work?

Thanks,
Meltem

From: Chen, Lily (Fed) <lily.chen@nist.gov>

Sent: Monday, September 13, 2021 8:21 AM

To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>

Subject: Re: SHA-3 Development

Hi, Meltem,

I think it is a good idea. Before we start, let's try to talk with Jim Foti to see if there are some other venues and **how the last issue of *Journal of Research of NIST* is planned**. It sounds the schedule is extremely tight. The article is going to be "historical". We need time to think the angle we describe it

and which kinds of details shall be included. I am afraid that it is hard to finish in 2 weeks. What do you think?

Lily

From: "Sonmez Turan, Meltem (Fed)" <meltem.turan@nist.gov>

Date: Tuesday, September 7, 2021 at 11:54 AM

To: Lily Chen <lily.chen@nist.gov>

Subject: SHA-3 Development

Hi Lily,

Hope you are enjoying your annual leave.

Similar to the *Development of the Advanced Encryption Standard* by Miles Smid, can we submit a paper to the Journal of Research for *SHA-3 development*? It might be a good publication to summarize the standardization process.

The final issue of *Journal of Research of NIST* accepts submissions through September 30, 2021.

If this is fine with you, I plan to communicate with previous project members and see who would want to contribute.

Thanks,
Meltem